To Follow or Not to Follow: A Study of User Motivations around Cybersecurity Advice

Usable-security researchers have long pondered what motivates some users to ignore advice and make decisions that appear to put their security and privacy at risk. The study reported here specifically investigated user motivations to follow or not follow computer security advice, through a survey distributed via Amazon Mechanical Turk. To guide the study design, the authors used a rational-decision model and current thought on human motivation. The data shows key gaps in perception between those who followed the tested pieces of advice (update software, use a password manager, use two-factor authentication, or change passwords) and those who did not and helps explain the participants’ motivations behind their decisions. Notably, the study found that social considerations were broadly trumped by individualized rationales.

User perceptions and adoption of various security tools and techniques has remained a popular research topic. Some studies have identified and others have attempted to explain a divergence between recommended actions and actual protections used by the public. This question of why some people follow security advice, while others do not, has been touched on before. However, to the best of our knowledge, it has not been broadly approached using empirical data collected and analyzed for that purpose.

We investigated the motivations of users to follow or not follow common computer security advice. Users’ decision making was modeled using a cost–benefit framework, with the concepts of risk and social motivation added. On the basis of this investigation, we present the findings from a web-based survey constituting both qualitative and quantitative data that was distributed to and completed by 290 Amazon Mechanical Turk users.
As a foundation for our survey, we used four common security recommendations: updating software, using a password manager, using two-factor authentication (2FA), and changing passwords. For each piece of advice, we formed two types of groups: those who followed the advice (Yes groups) and those who did not (No groups). We then compared their perceptions. Before collecting and analyzing data, we hypothesized that the benefits, costs, and risks of following and not following each piece of advice would be rated in a way that agreed with the participants’ reported decision to follow or not follow the advice. Additionally, we expected that social motivations would be rated lower than individual motivations.

These hypotheses were largely correct. The benefit of not following was rated higher by those who didn’t follow each piece of advice, whereas the risk of not following was rated higher by those who did follow each piece of advice. Furthermore, the cost of not following was seen as higher by those who followed each piece of advice compared to those who did not, for all the pieces of advice, except using 2FA. These findings indicate that each group viewed its decisions as the rational one, as we expected. Finally, individual concerns were rated higher than social concerns for all variables, indicating low social motivation around computer security.

BACKGROUND

Although complex, human decision making can be viewed as a consideration of cost and benefit, in which humans are rational actors who choose to minimize cost and/or maximize benefit. Herley highlighted this model in his work exploring the motivations around following security advice, citing the low chance of a security breach for any given user (representing low benefit) and the high cost of daily security maintenance.\(^4\) He also suggested that more data is needed to determine the actual cost and benefit of these decisions to better inform the advice experts give. Another study showed that users show rational tendencies when considering whether to accept advice, such as looking to the trustworthiness of the source in some cases (e.g., antivirus software), but relying on personal evaluation in others (e.g., passwords).\(^7\) Inspired by these prior efforts, we used a cost–benefit framework as the starting point for our study’s design.

In addition to cost and benefit, the literature shows us that risk perception is central to security-related behavior.\(^5,8\) Literature surveys have identified security risks and risk perceptions as key considerations in many studies that focus on psychology and computer security.\(^5\) The study designs of recent usable-security research have focused on risk as well.\(^2,9\) Thus, we incorporated perceptions of risk along with cost and benefit.

Although risk perception is intrinsically linked with security decisions, we also added social motivations (motivations driven by values or wanting to help or please others), which are argued to be independent of and much stronger or longer lasting than instrumental motivations (motivations related to gaining material reward or avoiding material cost).\(^10\) Some researchers have investigated social motivations in the area of usable security. For example, Das et al. found that users could be better motivated to act securely online if their peers would know the decisions they were making.\(^11\) Therefore, our study’s model was expanded to include how participant users thought their decisions affected users of other computers.

Finally, there is evidence in the literature suggesting that experts and average users think and act differently when it comes to computer security. Ion et al. showed that experts and regular users reported different behaviors when asked which they think are the best for staying safe.\(^1\) Additionally, another study found that security-sensitive users (as many experts arguably are, on the basis of their security-conscious behavior reported in Ion et al.’s study) and general users differ in their sources of security advice.\(^12\) However, Kang et al. found that there was no direct correlation between participants’ technical background and the actions they took to control their privacy.\(^2\) Thus, rather than separating users into experts and nonexperts, we simply compared those who followed each piece of advice with those who did not, to identify differences in perceptions between those two groups.
**METHODS**

As the previous section described, our study was designed to investigate the motivations of users to follow or not follow common computer security advice, using several cues from prior studies. We focused on four pieces of common security advice harvested from Ion et al.’s 2015 paper:\(^1\)

- keeping software up to date,
- using a password manager,
- using 2FA, and
- changing passwords frequently.

For each, we sampled two groups of users: those that followed the advice and those that did not. To help in describing the study, we refer to the samples of users who followed each piece of advice as Yes groups, whereas we refer to the samples of users who did not follow the advice as No groups. All groups were sent a similarly designed survey to gauge their motivations.

**Survey Content**

We extended the traditional cost–benefit analysis to include the perception of risk and consider the social aspect of each decision. These concepts were formalized into the following 12 variables:

1. Individual Benefit of Following
2. Social Benefit of Following
3. Individual Cost or Inconvenience of Following
4. Social Cost or Inconvenience of Following
5. Individual Risk of Following
6. Social Risk of Following
7. Individual Benefit of Not Following
8. Social Benefit of Not Following
9. Individual Cost or Inconvenience of Not Following
10. Social Cost or Inconvenience of Not Following
11. Individual Risk of Not Following
12. Social Risk of Not Following

Variables were defined using survey instruments phrased differently for each piece of advice, Yes or No group, and specific variable. One of these two phrasings was used to define each variable:

- **Phrasing A.** How much would you say [you | users of other computers] are [benefited | cost or inconvenienced | put at risk] by you (not) [following the advice]?
- **Phrasing B.** How much would you say [you | users of other computers] would be [benefited | cost or inconvenienced | put at risk] if you did (not) [follow the advice]?

Variables 1 through 6 were defined using Phrasing A for the Yes groups and Phrasing B for the No groups. Variables 7 through 12 were defined with Phrasing B for the Yes groups and Phrasing A for the No groups. This was done to match the instrument’s phrasing to the participant’s reported decision. Individual variables used “you” in the first bracket, whereas social variables used “users of other computers.” The second brackets were likewise replaced for the variables that asked about benefit, cost or inconvenience, and risk. Finally, “follow (or following) the advice” was replaced as appropriate for each piece of advice that we tested in the surveys (e.g., “use (or using) 2FA”), with “not” being added as needed.

Because each variable was defined in a slightly different format for the Yes and No groups, our analysis compared ratings that were more or less hypothetical, depending on the group. The goal of this work was to identify the possible gaps in perceptions between those who followed the security advice and those who did not.
For the decisions examined in this study, because the users might have been pondering a behavior they had not practiced in the past, at least some of their considerations might have been hypothetical. Their perceptions of possible outcomes might have been skewed or biased, which we hoped to identify. Therefore, our study had to compare hypothetical ratings with more grounded reports.

A 4-point Likert scale was used for each of the quantitative questions described above (i.e., 1 = none, 2 = little, 3 = some, and 4 = a lot). An open-ended statement requesting survey takers to indicate why they chose to follow or not follow the target advice (“Please explain in a few sentences why you choose to (not) [follow the advice]”) was shown to participants first, on a separate page in all surveys. We did this to avoid biasing the open-ended responses toward our overall study framework.

The quantitative questions were then divided into two additional pages in the survey. The first asked about perceptions of the participant’s reported behavior; the second asked about perceptions of the opposite behavior.

Survey templates for both groups, showing the format, are in the appendix of our 2016 SOUPS (Symp. Usable Privacy and Security) paper.3

**Sampling Methodology**

We used Mechanical Turk to gather an initial sample of participants who answered a screening survey that asked for basic demographic information as well as a report of which of our study’s advice they did or did not follow. Participants were compensated $0.25 for completion of these instruments. This compensation level was set low owing to the small number of instruments included. Participants were informed that they could be contacted with an additional survey based on their responses to this initial set of instruments, but no indication was given as to how eligibility would be determined.

On the basis of the screening survey responses, we formed the Yes and No group for each piece of advice by randomly selecting 50 participants that matched the group’s target behavior. For example, the Yes group for updating comprised a random selection of 50 respondents who said they updated on the initial survey. A participant selected to be in a group was not considered for inclusion in others.

Follow-up participants were contacted with the appropriate survey through Mechanical Turk’s messaging system. They were informed that their continued participation was entirely voluntary. If they chose to continue, they were compensated another $4 for their time and effort on the longer survey. Not all 50 for each group replied, resulting in samples between 30 and 40 participants for each, for a total of 290 across all eight groups.

**EVALUATION**

Our analysis was guided by our study model framework. We identified gaps in perceptions between the Yes and No groups for each piece of advice, with particular divergence around the benefit and risk associated with their decisions. Our qualitative data helped us understand some possible explanations for the differences between groups. Finally, we revisited the quantitative data to highlight the dominance of individual considerations around deciding to follow computer security advice.

**Gaps in Perceptions**

Before data collection, we hypothesized that the participants’ ratings would align with their reported behavior. Those who didn’t follow each piece of advice were expected to rate the risk and cost of doing so as lower than those who did follow the advice, while also rating the benefit higher. Conversely, those who did follow the advice were each expected to rate the benefit as
higher than those who didn’t follow the advice, while rating the risk and cost of doing so as lower.

Through analysis of the data, we saw significant gaps in the rated benefit, cost, and risk involved in the decision to follow each piece of advice, when comparing the Yes and No groups that generally agreed with our hypothesis. Table 1 shows summaries of responses for each variable, from each piece of advice’s Yes and No groups, along with Mann-Whitney U tests comparing the distribution. We used Cohen’s $d$ to express the effect size of the difference between the Yes and No groups’ distributions.

Table 1. Rating summaries for all variables, from each group, with U tests comparing the distribution between each Yes group (participants who followed the advice) and No group (participants who did not follow the advice). The effect size is measured with Cohen’s $d$. A shaded background indicates results that are of significance $p < 0.004$.

<table>
<thead>
<tr>
<th></th>
<th>Of following</th>
<th>Of not following</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>Avg. (Md.)</td>
<td>Avg. (Md.)</td>
</tr>
<tr>
<td>Update</td>
<td>3.77 (4)</td>
<td>2.97 (3)</td>
</tr>
<tr>
<td>PW mgr.</td>
<td>3.78 (4)</td>
<td>2.50 (2.5)</td>
</tr>
<tr>
<td>2FA</td>
<td>3.71 (4)</td>
<td>2.90 (3)</td>
</tr>
<tr>
<td>Change PW</td>
<td>3.47 (4)</td>
<td>2.53 (3)</td>
</tr>
<tr>
<td>Social benefit</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Update</td>
<td>2.71 (3)</td>
<td>2.39 (3)</td>
</tr>
<tr>
<td>PW mgr.</td>
<td>2.08 (2)</td>
<td>1.70 (1)</td>
</tr>
<tr>
<td>2FA</td>
<td>2.48 (2)</td>
<td>2.29 (2)</td>
</tr>
<tr>
<td>Change PW</td>
<td>1.73 (1)</td>
<td>1.48 (1)</td>
</tr>
<tr>
<td>Individual risk</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Update</td>
<td>1.56 (2)</td>
<td>1.72 (2)</td>
</tr>
<tr>
<td>PW mgr.</td>
<td>1.83 (2)</td>
<td>2.53 (2)</td>
</tr>
<tr>
<td>2FA</td>
<td>1.56 (1)</td>
<td>1.62 (1)</td>
</tr>
<tr>
<td>Change PW</td>
<td>1.35 (1)</td>
<td>1.71 (2)</td>
</tr>
<tr>
<td>Social risk</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Update</td>
<td>1.13 (1)</td>
<td>1.38 (1)</td>
</tr>
<tr>
<td>PW mgr.</td>
<td>1.41 (1)</td>
<td>1.53 (1)</td>
</tr>
<tr>
<td>2FA</td>
<td>1.31 (1)</td>
<td>1.48 (1)</td>
</tr>
<tr>
<td>Change PW</td>
<td>1.19 (1)</td>
<td>1.17 (1)</td>
</tr>
</tbody>
</table>
Benefit can be a key motivator if a decision appears to provide it. Our study measured both the rated benefit of following and not following each piece of advice. By comparing these benefit ratings between the Yes and No groups, we could see whether the participants diverged in their perceptions of the benefit related to each piece of advice.

As seen in Table 1, for all pieces of advice, the Yes groups rated the benefit of following the advice as significantly higher than the No groups rated the benefit they thought they would get if they followed the advice. Social Benefit of Following was not rated significantly differently between groups for any piece of advice.

We found a similar, but mirrored, tale for Individual Benefit of Not Following. In this case, the No groups rated their benefit as significantly higher than the Yes groups rated the benefit they would experience if they no longer followed the advice. Again, there were no significant differences between groups on any piece of advice for Social Benefit of Not Following.

When we looked at the qualitative data to help explain this gap, a few patterns emerged across the pieces of advice. About half of those who said they updated frequently and half who said they used a password manager mentioned the added security benefit as a reason for their decision. Furthermore, 72% \((N = 36)\) of those who used 2FA and 86% \((N = 37)\) of those who frequently changed their password mentioned security benefits in their comments. Some decisions seemed to have other benefits as well, such as getting the latest software through updating (10 of the 39 participants who updated regularly) or the added convenience of a password manager (37 of the 40 password manager users).

Risk

Decisions related to security are uniquely tied to risk. So, we dug into the participants’ ratings of the risk involved in and avoided by their security decisions, to better understand their thinking. Looking at Table 1, for all or most advice, Individual Risk of Not Following and Social Risk of Not Following were rated lower by the No groups than by the Yes groups.

Many comments from the No groups mentioned a lack of worry about the risk as a reason for their decision. About a fifth of comments from both those who did not use 2FA (19%) and did not change passwords regularly (18%) said they decided not to follow the advice because they didn’t care if they were hacked.
Sometimes, rather than not caring about a risk, participants in the No groups expressed heightened attention to the perceived risk, which impacted their decision. For example, eight comments from those who did not update said they wanted to avoid change or harm. Notably, almost half (45%, $N = 38$) of those who did not use a password manager said they were explicitly avoiding a security risk they saw in using such a tool. We also see this sentiment in Table 1, where the password manager No group rated Individual Risk of Following as significantly higher than the Yes group. In fact, Individual Risk of Following was rated significantly differently between the Yes and No groups only for using a password manager; no other advice had significant differences for this variable.

The No group’s qualitative comments shed some light. Twelve of the 38 comments mentioned avoiding centralization of passwords as a reason for deciding to not use a password manager. The Yes groups showed a pattern of being motivated by a security benefit or avoidance of risk; ironically, many from the password manager No group were similarly motivated in their counter-decision.

Cost

No matter how prominent the risk being avoided, if the cost is too high, many users will refuse or be unable to follow the advice. Thus, we analyzed how participants from each group rated the cost of following and not following each piece of advice.

For updating frequently and using a password manager, the Yes groups rated Cost of Not Following as higher than the No groups for both the individual and social phrasings. Additionally, the individual phrasing was rated significantly differently for changing passwords. Over half (56%, $N = 39$) of the comments from those who updated reported avoiding bugs as a reason for their action. The large number of comments from the users of password managers that mentioned the convenience of the tool showed how advice-specific implications can alter decision making for some users.

Cost was a top complaint from the No groups. Almost a quarter (23%, $N = 30$) of those who didn’t update, half (48%, $N = 31$) of those who didn’t use 2FA, and over half (53%, $N = 38$) of those who didn’t frequently change passwords said the avoidance of an inconvenience influenced their decision. For not using 2FA, 23% ($N = 31$) mentioned avoiding a cost explicitly, while 39% ($N = 38$) of those who did not frequently change passwords said they made their decision because frequently changing passwords would be hard to remember to do or make their passwords hard to remember. These findings highlight how the context of a decision, specifically the cost involved, might have a big impact on a user’s action.

Social versus Individual Motivations

Although many comments from the participants at the start of the survey conformed to the benefit–risk–cost breakdown in our study’s framework, the social–individual divide was not as apparent. Only 13 of the 290 comments we received mentioned any kind of social motivation, all from the Yes groups. Prompted by this and our study hypothesis that the individual ratings would be higher than the social ratings, we used the quantitative data to investigate further.

Figure 1 shows the relative magnitude of the ratings for the individual phrasings of each variable compared to the social phrasings. The individual phrasings were rated consistently higher for all, regardless of the advice or decision. Statistical tests of these differences showed that they were significant.
DISCUSSION

Participants in our study generally rated the benefit, risk, and cost around each decision in a way that agreed with their reported behavior, which we expected in our hypotheses. For example, for all advice, Benefit of Following was rated higher for the Yes groups than the No groups, while Benefit of Not Following was rated higher by the No groups. This generally followed for risk and cost as well, where the Yes groups were apt to rate the risk and cost avoided by their decision as higher than the No group. This trend should be unsurprising, as you would expect an adherent to think he or she is getting more benefit (or avoiding more cost and/or risk) than a nonadherent. However, it is important to keep in mind that those you are advising might have a different outlook than you. So, it is imperative for the advice experts give to be provably effective and usable because they must be convincing when trying to motivate new behavior.

Notably, for most (but not all) advice, Individual Costs of Following and Individual Risks of Following were not rated significantly differently between the Yes and No groups. This could indicate that the groups agreed on the cost and risk of following those pieces of advice. This evidence adds credence to calls from others that at least some users ignore security advice because of high cost and/or low benefit. In our sample, benefit was generally rated differently, whereas cost was rated much more similarly between the Yes and No groups. Although more data is certainly needed, it could be that some who do not adhere to good security practice do not see a usability issue in following the advice (as indicated by their agreement with the Yes groups on cost), but have a different perspective on the risk of their inaction and/or the efficacy of solutions.

Our participants agreed in another way across the Yes and No groups: their motivations were predominately individual rather than social, another result we expected in our hypotheses. We saw this trend in both the quantitative and qualitative data, and it makes sense when you consider the individualized aspects of using a computer. Many times, individuals are physically alone when using their devices, which could impart a sense of isolation, even when on the Internet.
Although the participants did not identify it, their computer security decisions do affect others. For example, if a user chooses not to update, causing his or her device to be compromised and assimilated into a malicious botnet through a security flaw, then that user’s decision not to update could impact others when their device participates in a distributed attack. Although newer research has pointed to the power of social motivation,\(^\text{10}\) given the lack of social consciousness around security decisions, future work that attempts to motivate users through social motivation needs to rethink how to best approach the problem.

Finally, it is interesting to note that, on the basis of the project from which they were extracted, three pieces of the advice tested in this study were commonly recommended by experts, whereas the fourth (changing passwords frequently) was not commonly recommended by experts but was still regularly cited by average users as a way to stay safe online (i.e., folk advice).\(^\text{11}\) Looking at our data, there are some trends that differentiated the folk advice from expert advice. Specifically, frequently changing passwords seemed to offer the least benefit while simultaneously being the costliest, as can be seen in the ratings summaries of Table 1. Interestingly, this trend held for both the Yes and No groups, showing another area in which, despite a divergence in behavior, the participants did not disagree in their ratings.

Identifying why, despite lower efficacy and higher cost, some users still gravitate toward folk advice such as changing passwords, while balking at many expert recommendations, is imperative to understand their decision making in this space. For example, some users might get their security habits from the IT policies of their workplace, which commonly suggest or require regular password changes, highlighting a subtle channel of communication (i.e., corporate IT policy) security experts might be able to utilize to increase secure behavior. Further investigation is needed to better inform these findings.

Our approach is not without limitations. For instance, although we were able to find statistically significant differences in many places, more data from more users could generate additional findings or new insight into existing findings. Larger samples could garner stronger effect sizes than those in this study, which were generally moderate. In addition, examination of more types of advice and contexts (e.g., perceptions of the benefit, risk, and cost of specific kinds of devices) could also broaden the picture. An expanded decision-making framework might provide more insight but would likely require a study larger than that presented here, introducing different limitations. Finally, because Mechanical Turk’s population is not representative of the general population, replication of this study with more samples would help generalize the findings.

CONCLUSION

Our results show differences in the perceptions of benefit, risk, and cost associated with the decision to adhere to a variety of recommended security behaviors. Both those who did and did not follow each piece of advice reported that their decision provided them more benefit than if they changed. Those who followed the advice rated the risk of changing their decision as much higher than did those who did not follow the advice. The cost of not following the advice was also seen as higher by those who followed it than by those who did not. Finally, we found that individual concerns were rated consistently higher than social concerns.

More data about the actual risk and cost incurred by users as well as further investigations into perceptions will serve to better frame and explain the findings of this study. Nonetheless, our results have provided insight into user motivation in this context and serve to inform future efforts toward the broader goals of the usable-security field.

ACKNOWLEDGMENTS

This work is supported by the US National Science Foundation under grant CNS-1343766 and by GAAAN (Graduate Assistance in Areas of National Need) Fellowship P200A130153. Any opinions, findings, or recommendations expressed are those of the authors and do not necessarily reflect the views of the funding agencies.
REFERENCES


ABOUT THE AUTHORS

Michael Fagan is a recent PhD graduate from the University of Connecticut’s Computer Science and Engineering Department. His research interests include the human factors of cybersecurity and adoption of secure behaviors, particularly human motivations when making risk-associated decisions. Fagan received a BA in history and computer science from Vanderbilt University. Contact him at michael.fagan@uconn.edu.

Mohammad Maifi Hasan Khan is an associate professor in the University of Connecticut’s Computer Science and Engineering Department. His research interests include usable cybersecurity, risk communication, trust in automation, and performance modeling and troubleshooting of large-scale systems. Khan received a PhD in computer science from the University of Illinois, Urbana-Champaign. Contact him at maifi.khan@uconn.edu.